UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,224	02/26/2004	Burkhard Kuhls	080437.53236US	2832

23911 7590 09/29/2010
CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
09/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/786,224	**Applicant(s)** KUHLS, BURKHARD	
	Examiner CARLTON V. JOHNSON	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. The action is in response to application amendments filed on 7-13-2010.

2. Claims **1, 3 - 9, 12 - 20** are pending. Claims **1** has been amended. Claim **2, 10, 11** have been cancelled. Claims **1, 7, 19** are independent. The application was filed on 2-26-2004.

Response to Arguments

3. Applicant's arguments have been fully considered but they were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, *software signature certificate is an operating system-level component. (Remarks Page 7)*

There does not appear to be any disclosure in the claimed invention that a certificate (of any type) is an operating system-level component. England does disclose that a certificate can be used as an authentication tool for an operating system and its components (software components).

The previous claim limitation "before its use" is equivalent to the newly amended claim limitation "wherein prior to execution of the software". The software is still protected by a digital signature that can be verified. England discloses that the signature of the boot block is checked before loading the digital rights OS. The software is checked for integrity before its usage as a digital rights OS. (see England col 9, lines 7-10: digital rights OS; col 8, 48-51:system incorporates public/private key pairs, digital certificates;

col. 8, lines 34-37: boot block signed by OS manufacturer; (boot block processed before execution or use of software); col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate)

England also discloses utilizing certificates with public and private key pairs with certificates to verify a digital signature.

In addition, England does disclose checking a signature certificate for integrity.

For additional clarity, England discloses a certificate is signed, therefore the certificate can be checked for validity by checking its digital signature. (see England col. 8, lines 7-14: certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

3.2 Applicant argues that the referenced prior art does not disclose, *a control unit. (Remarks Page 9)*

England discloses a control entity or a control unit. (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer digitally signs software before use; private (secret) key of manufacturer's CPU (control entity)) And, Wong explicitly discloses a control unit for an automobile or vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: control unit; software for vehicle control unit)

England discloses the Claim 7 limitations: 1. a clearing code site signature; 2. a software signature certificate; 3. clearing code data and their signature; and 4. software and its signature. England discloses a certificate (software signature, clearing code signature) which contains a public/private key pair for each particular certificate. England also discloses (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU; certificate contains public key)

England discloses the clearing code data (identity) and signature capability for a certification (clearing code certificate. (see England col. 8, lines 26-28; col. 9, lines 4-10: software identity; identify of an authenticated OS)
This is equivalent to the specification on page 3, paragraphs [0010] and [0012], which discloses that the clearing code certificate contains an identifier and the capability to restrict usage to a particular control entity.

3.4 Applicant argues that the referenced prior art does not disclose, *checks whether a software signature certificate and signed software has been changed or manipulated.*

England discloses a verification step to determine whether signed software has been changed or manipulated. A certificate (no matter what type) is still digital information and its integrity can be checked using digital signature verification procedures. England discloses the verification of whether digital information (a digital certificate) has been modified or changed. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised) The Examiner is operating under the assumption that when a component is signed then the component is protected. Any modification or updates to the certificate can be discovered by checking the digital signature.

The Examiner must reiterate that checking the validity of a signature does indicate whether an entity (component, digital certificate) has been changed or manipulated since the generation and attachment of a digital signature. If a component is updated, then the digital signature is updated and reattached to the document after update procedure.

3.4 Applicant argues *dependent claims 3-6, 9, 12-18, 20*

Responses to arguments against independent claims answer arguments against associated dependent claims.

3.5 Ishii discloses the generation of a signature (a standard cryptographic processing function) using a public key of one entity and a secret key of another entity. (Ishii col 5, lines 43-67: signing (signature certificate) by using the secret key of certification issuing center (first public key cryptosystem); deciphering processing using the secret key or encryption processing (signature generation) using the public key or the second public key cryptosystem; cryptographic processing (signature generation using a public key and a secret key)

The specification on page 6, paragraph [0021] discloses that the software signature site is the manufacturer of the software and that the manufacturer of the software is also the manufacturer of the control unit or entity. England discloses a manufacturer of software. And, England discloses that the software manufacturer signs the software (such as a boot block). Since it is the manufacturer of the software (England discloses) therefore it is the software signature site as per specification. In addition, England discloses that the manufacturer has a public/private key pair. That particular private key is used to sign the software. (see England col. 7, line 63 - col. 8, line 37: manufacturer (CPU, controlling entity for control unit, OS software manufacturer) certificate generated with public/private keys; manufacturer's public/private key pair)

England discloses a software signature site and a public/private key pair used for signing software. (see England col. 7, line 63 - col. 8, line 37: manufacturer (CPU, control entity, OS software manufacturer) certificate generated with public/private keys; manufacturer's public/private key pair)

3.6 England prior art discloses a trusted third party and the third party key are used to sign software. (England col. 8, line 66 - col. 9, line 3: components signed by a trusted third party)

Ishii discloses the generation of a signature (signature certificate) using a public key of one public key cryptosystem and a public key of a second public key cryptosystem used for cryptographic functions such as signature generation.

And, Wong discloses a vehicle control unit and controlling a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

Claim Rejections – 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 3 - 20** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **England et al.** (US Patent No. **6,330,670**) in view of **Ishii** (US Patent No. **5,768,389**) and further in view of **Wong et al.** (US Patent No. **5,957,985**)

Regarding Claim 1, England discloses a method comprising providing software for use by a control unit;

b) wherein prior to execution of the software, by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; (boot block processed before execution or use of software); col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer digitally signs software before use; private (secret) key of manufacturer's CPU (control entity)), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair (public/private keys) generated and used)

Furthermore, England discloses:

c) checking the signed software signature certificate for integrity, according to a public key method using a public key of the trust center; (see England col. 8, lines 7-14: certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 8, line 66 - col.9, line 3: trusted third party (use digital signature for authentication); trusted third party equivalent to trust center)

d) checking the signed software for integrity, using a public key of the software signature site contained in the software signature certificate, the public key of the software signature site being complementary to the secret key of the software signature site; (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; col. 11, lines 54-59: checks digital signature of a component before loading it; signature valid then component has not been compromised and loaded)

The digital rights OS components are loaded and the digital signature is checked for each component before loading. And, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software.
This is equivalent to disclosure in the specification on page 6, paragraph [0021], lines 3-6, that discloses a software signature certificate is generated and signed by the manufacturer of software.

England does not specifically disclose generating a certificate using a public key and a secret key.

However, Ishii discloses for a): wherein generating a software signature certificate using the public key of the software signature site and a secret key of a control entity, according to a public-key method. (see Ishii col 5, lines 43-67: signing (signature certificate) by using the secret key of certification issuing center (first public key cryptosystem); deciphering processing using the secret key or encryption processing (signature generation) using the public key or the second public key cryptosystem; cryptographic processing (signature generation using a public key and a secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key and a secret key as taught by Ishii. One of ordinary skill in the art would have been motivated to employ the teachings of Ishii for the added protection of a key and certification mechanism that is physically and electronically protected such that tampering cannot be done in any way whatsoever. (Ishii col 7, ll 14-18)

England-Ishii does not specifically disclose a control unit of a vehicle.
However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: control unit; software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-Ishii for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for usage of a commonly accepted standard device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 3, England discloses the method according to claim 1, wherein one of a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. (see England col. 7, line 63 - col. 8, line 14: manufacturer (CPU, control entity) certificate generated; manufacturer public/private (secret) key pair usage)

Regarding Claim 4, England discloses the method according to claim 1, wherein clearing code data are signed using a secret key of a clearing code site according to a public key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private key pair usage)

Regarding Claim 5, England discloses the method according to claim 1, wherein a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private (secret) key pair usage)

Regarding Claim 6, England discloses the method according to claim 3, wherein the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (protected area of memory); col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

Regarding Claim 7, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) before its use by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; sign boot code), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer signs software), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair (public/private keys) generated and used; public key of manufacturer for CPU (control entity))

Furthermore, England discloses the following:

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) wherein a clearing code site signature certificate, a software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU; certificate contains public key)

Furthermore, England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party)
This is equivalent to the disclosure in specification on page 6, paragraph [0022], that a trust center or trusted third party generates certificates.

England does not specifically disclose software signature certificate is generated using the public key of the software signature site and a secret key of a control unit. However, Ishii discloses wherein generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public-key method. (Ishii col 5, lines 43-67: signing (signature certificate) by using the secret key of certification issuing center (first public key cryptosystem); deciphering processing using the secret key or encryption processing (signature generation) using the public key or the second public key cryptosystem; cryptographic processing (signature generation using a public key and a secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key and a secret key as taught by Ishii. One of ordinary skill in the art would have been motivated to employ the teachings of Ishii for the added protection of a key and certification mechanism that is physically and electronically protected such that tampering cannot be done in any way whatsoever. (Ishii col 7, ll 14-18)

England-Ishii does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-Ishii for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 8, England discloses the method according to claim 1, wherein the software signature certificate includes at least one validity restriction. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

Regarding Claim 9, England discloses the method according to claim 5, wherein the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to an identification number. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); uniquely determines the OS; col. 8, line 66

- col. 9, line 3: trusted third party to digitally sign all components)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 12, England discloses the method according to claim 5, wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 13, England discloses the method according to claim 4, wherein the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 14, England discloses the method according to claim 1, wherein the control unit is equipped with a sequence-controlled microprocessor that implements one of the above-described methods.

England does not specifically disclose a motor vehicle control unit.

However, Wong discloses a motor vehicle control unit. (see Wong col. 2, lines 21-29: vehicle processor (microprocessor); col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle control unit as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 15, England discloses a control unit, which implements a method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 16, England discloses a data processing system, which implements a method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 17, England discloses a computer program product sequence control of a data processing system, which implements the method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle or motorcycle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle or motorcycle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 18, England discloses a data carrier, comprising a computer program product according to claim 17. (see England col. 10, lines 55-59: software; computer program product)

Regarding Claim 19, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) storing, a software signature certificate; receiving, signed software; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) checking, whether the software signature certificate has been changed or manipulated; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) checking, whether the signed software has been changed or manipulated. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 20, England discloses the method of claim 19, further comprising:

a) storing, a trust center certificate that includes a public key and a signature generated using a secret key of a trust center; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) storing, a clearing code site signature certificate that includes a second public key and a second signature; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

c) wherein the software signature certificate includes a third public key and a third signature; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
September 13, 2010